UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,116	03/14/2001	Akiko Kawamoto	Q63597	1497

7590 04/20/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3202

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,116	KAWAMOTO, AKIKO	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/14/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-3, 5-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra (US 5,748, 736), and further in view of Roden (US 5,970,477).

a. *Referring to claim 1:*

i. Mittra teaches:

(1) a sender terminal for transmitting multicast data; a receiver terminal for receiving multicast data; an authentication server processor for managing the sender terminal and the receiver terminal **[i.e., referring to Figure 1, the system of Mittra's invention implements a secure multicast group (the "group") consisting of senders, receivers, a group security controller (GSC), and some number of trusted intermediary (TI) servers. The GSC and each TI server are responsible for maintaining the security of the group by authenticating and authorizing all other members of the multicast as well as managing the group keys (Kgrps) that are used to encrypt the messages multicast to the group (column 4, lines 8-16). In addition, in each embodiment of the inventive system, each GSC, TI server, sender, and receiver is a device, and all such devices are programmed in such a manner that the system can implement a secure multicast. For example, each receiver, sender, GSC, and TI can be a programmed personal computer including a network connection (e.g., to the Internet), and each GSC or TI can be a programmed processor including router circuitry (column 6, lines 45-52)];**

(2) a first user processor provided in the sender terminal for transmitting a login requirement to the authentication server processor; and a second user processor provided in the receiver terminal for transmitting a login requirement to the authentication server processor **[i.e., joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line). The purpose of the secure channel is to facilitate and isolate confidential communication between the GSC and this member during the time that the member is part of the group. Upon receiving a join request (and approving it), the GSC inserts the member's identification and information concerning the secure channel in a private database it maintains. In this way the GSC has full knowledge of the group membership and can communicate with each member separately and securely when required. The member must also store information concerning the secure channel for future communication with the GSC. Only the GSC maintains information concerning group membership; members do not know about each other (except that receivers may need to know the list of authorized senders). However, it should be noted that the invention does not protect against traffic analysis as a method of gaining information about group membership. The secure channel can be set up using any of the authentication protocols that are well known in the literature that provide mutual authentication and the exchange of a secret (i.e., a key) that can be used to encrypt farther communication between the GSC and this member (which is either a user of the sender device or a user of the receiver device) (column 7, line 45 through column 8, line 7)]**,

ii. Although Mittra teaches the claimed subject matter and as well as the termination of the group membership **(column 8, line 41-44)**, Mittra does not explicitly mention:

(1) wherein the authentication server processor executes a logout when the second user processor in the receiver terminal does

not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

iii. On the other hand, Roden teaches:

(1) If the received message does not includes the correct key, the "NO" branch is followed to step 605 in which the point of presence 22 responds to a potential fraudulent message. For example, the communication may be disconnected **(column 17, lines 35-39).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Roden into Mittra so as to measure system security **(column 4, line 60 of Roden).**

v. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matchett into Davis since a unique key, such as a randomly generated number, may be used as a security device **(column 5, lines 31-32 of Roden).**

b. *Referring to claim 2:*

i. Mittra further teaches:

(1) wherein the sender terminal encrypts multicast data and transmits encrypted multicast data to the receiver terminal when the first user processor transmits the login requirement to the authentication server processor and when the authentication server processor permits login **[i.e., once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission (column 8, line 15-18)].**

c. *Referring to claim 3:*

i. Mittra further teaches:

(1) wherein the receiver terminal registered in the authentication server processor decrypts encrypted multicast data using an encryption key distributed from the authentication server processor and receives decrypted multicast data in an application provided in the receiver terminal when the second user processor transmits the login requirement to the authentication server processor and when the authentication server processor permits login **[i.e., once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission (column 8, line 15-18)].**

d. *Referring to claim 6:*

i. Mittra further teaches:

(1) wherein the second user processor transmits a logout requirement to the authentication server processor and the authentication server processor terminates user management when multicast data communication is terminated in an application in the receiver terminal **[i.e., in the case, the member voluntarily wishes to disconnect/logout and needs to notify the GSC of its intention so that the GSC may change the Kgrp and then provide a confirmation to the leaving member (column 8, lines 38-41)].**

e. *Referring to claim 7:*

i. Mittra further teaches:

(1) an authentication server processor; a first receiving section for receiving a login requirement transmitted from a first user processor provided in a sender terminal which transmits multicast data; a second receiving section for receiving a login requirement transmitted from a second user processor provided in a receiver terminal which receives multicast data; and a user registration information section for registering user's individual information, wherein the user uses the sender terminal, the sender terminal which is permitted login by the authentication server processor encrypts multicast data and transmits encrypted multicast data, and the receiver terminal, which is

registered as a user in the user registration information section by the authentication server processor, is permitted login and receives multicast data **[i.e., this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above. Thus, joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line). The purpose of the secure channel is to facilitate and isolate confidential communication between the GSC and this member during the time that the member is part of the group. Upon receiving a join request (and approving it), the GSC inserts the member's identification and information concerning the secure channel in a private database it maintains. In this way the GSC has full knowledge of the group membership and can communicate with each member separately and securely when required. The member must also store information concerning the secure channel for future communication with the GSC. All communications from the GSC must include a message digest and be digitally signed so that receivers may verify that the message has not been corrupted and the sender was actually the GSC (column 7, lines 46-59). In addition, if the access point is at a level such that the joining member contacts not the GSC but a parent TI server (e.g., in the case that receiver 114f of Figure 1 seeks to join the group consisting of all elements of Figure 1 other than receiver 114f, in which case receiver 114f would contact TI server 115c rather than GSC 111), the TI server performs authentication on behalf of the GSC and changes the Kgrp (for its sub-group) using the above-described procedure performed by the GSC (to perform authentication and change the Kgrp). However, in order to do this, the TI server in turn must first be registered with its parent TI server or the GSC. If it is not, the TI server performs a registration with its parent TI server (or the GSC) prior to registering the joining member (column 13, lines 44-56)],**

ii. Although Mittra teaches the claimed subject matter and as well as the termination of the group membership **(column 8, line 41-44)**, Mittra does not explicitly mention:

(1) wherein the authentication server processor executes a logout when the second user processor in the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

iii. On the other hand, Roden teaches:

(1) If the received message does not includes the correct key, the "NO" branch is followed to step 605 in which the point of presence 22 responds to a potential fraudulent message. For example, the communication may be disconnected **(column 17, lines 35-39).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Roden into Mittra so as to measure system security **(column 4, line 60 of Roden).**

v. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matchett into Davis since a unique key, such as a randomly generated number, may be used as a security device **(column 5, lines 31-32 of Roden).**

f. *Referring to claims 8 and 9:*

i. These claims have limitations that is similar to those of claim 7, thus they are rejected with the same rationale applied against claim 7 above.

g. *Referring to claims 10-11:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

3. Claims 1, 4, and 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley et al (US 6,275, 859 B1), and further in view of Roden (US 5,970,477).

a. *Referring to claim 1:*

i. Wesley teaches:

(1) a sender terminal for transmitting multicast data; a receiver terminal for receiving multicast data; an authentication server processor for managing the sender terminal and the receiver terminal; a first user processor provided in the sender terminal for transmitting a login requirement to the authentication server processor; and a second user processor provided in the receiver terminal for transmitting a login requirement to the authentication server processor **[i.e., referring to Figure 1, a number of network nodes 10 are to become part of a multicast data distribution session. Included in the set of nodes 10 are a sender node 10-S and one or more receiver nodes 10-R1 through 10-RN. During the multicast session to be established, data packets are originated by the sender node 10-S and delivered to the various receiver nodes 10-R1 though 10-RN. Before joining a multicast session, each node 10 contacts a central authority or CA 12 to obtain the necessary credentials. The CA 12 is generally a separate network node that is responsible for managing access to the multicast session. The CA 12 may also be referred to as a channel manager or group controller. Each node 10 communicates with the CA 12 via a respective secure unicast channel 14 (shown as channels 14-S and 14-1 through 14-RN in Figure 1). Upon being contacted by a node 10, the CA 12 authenticates the node 10 via any appropriate means, which can include for example using signed certificates, passwords, or a registration process in which a prospective group member obtains a group identity after submitting payment information such as a credit card number. If the node 10 approaches the CA 12 with a digitally signed certificate, the CA 12 verifies the certificate by using the public key of the authority that signed the node's certificate.**

Thus, the CA 12 is responsible for maintaining or procuring on demand the public keys of all certificate-issuing authorities (column 3, line 50 through column 4, line 8)]

ii. Wesley teaches the claimed subject matter except for:

(1) wherein the authentication server processor executes a logout when the second user processor in the receiver terminal does not receive a periodically distributed encryption key which is periodically generated by the authentication server processor and distributed to the receiver terminal.

iii. On the other hand, Roden teaches:

(1) If the received message does not includes the correct key, the "NO" branch is followed to step 605 in which the point of presence 22 responds to a potential fraudulent message. For example, the communication may be disconnected **(column 17, lines 35-39).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the teaching of Roden into Mittra so as to measure system security **(column 4, line 60 of Roden).**

v. The ordinary skilled person would have been motivated to:

(1) have applied the teaching of Matchett into Davis since a unique key, such as a randomly generated number, may be used as a security device **(column 5, lines 31-32 of Roden).**

b. *Referring to claim 4:*

i. Wesley further teaches:

(1) wherein a receiver terminal, other than the receiver terminal registered in the authentication server processor, is rejected an encryption key distribution from the authentication server processor when the second user processor transmits the login requirement to the authentication server processor and when the authentication server processor rejects the login

requirement **[i.e., each participation certificate 16 also includes additional information such as starting and ending times for a period of authorized participation by the node 10, and/or an identifier of a role the node 10 may play in the multicast session (column 4, lines 21-26). In addition, each node 10 is responsible for using the information in the certificates 16 received from other nodes 10 to verify that the other nodes 10 are authorized to participate in the multicast session. In particular, a node 10 verifies that another node 10 advertising its ability to play a particular role, such as the role of repair node, is authorized to play such a role. A node 10 performs this verification by comparing the advertised ability with information in the certificate. Once the repair node and the receiver authenticate and verify each other's authorization, every control message exchanged henceforth between the two nodes is digitally signed. Digital signatures enable the nodes to accept and process only those messages that are produced by legitimate nodes, and to thus discard/reject messages from malicious nodes (column 4, lines 52-65)].**

c. *Referring to claims 7,8, and 9:*

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

d. *Referring to claims 10-11:*

i. These claims have limitations that is similar to those of claim 4, thus they are rejected with the same rationale applied against claim 4 above.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

TBT
April 13, 2005